Quantum Cryptography Approaching the Classical Limit

Christian Weedbrook,[1,2,*] Stefano Pirandola,[3] Seth Lloyd,[2,4] and Timothy C. Ralph[1]
[1]*Department of Physics, University of Queensland, St Lucia, Queensland 4072, Australia*
[2]*Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge MA 02139, USA*
[3]*Department of Computer Science, University of York, York YO10 5DD, United Kingdom*
[4]*Department of Mechanical Engineering, Massachusetts Institute of Technology, Cambridge MA 02139, USA*

(Dated: February 17, 2011)

We consider the security of continuous-variable quantum cryptography as we approach the classical-limit, i.e., when the unknown preparation noise at the sender's station becomes significantly noisy or thermal (even by as much as 10^4 times greater than the variance of the vacuum mode). We show that, provided the channel transmission losses do not exceed 50%, the security of quantum cryptography is not dependent on the channel transmission, and is therefore, incredibly robust against significant amounts of excess preparation noise. We extend these results to consider for the first time quantum cryptography at wavelengths considerably longer than optical and find that regions of security still exist all the way down to the microwave.

PACS numbers: 03.67.-a, 03.67.Dd, 03.67.Hk, 42.50.-p, 89.70.Cf

Introduction - Quantum key distribution (QKD) using continuous variables (CV) [1, 2] allows two people, Alice and Bob, to generate a secure key which can be used to encrypt messages. CV-QKD protocols using Gaussian modulation [3–8], initially begin with Alice preparing a number of randomly displaced pure coherent states and sending them over an insecure quantum channel to Bob. Generally, it is assumed that Alice's states must be pure quantum states to a good approximation otherwise her ability to perform QKD will rapidly become compromised. This seemed to be borne out by recent calculations [9] that showed that the distance over which CV-QKD was secure, when Alice used mixed coherent states in the protocol, fell rapidly as the states became significantly impure.

In this Letter, we show that, provided the channel transmission losses do not exceed 50 %, the security of quantum cryptography is not dependent on the channel transmission, and is therefore incredibly robust against significant levels of impurity of Alice's states, without the additional previous requirement of purifiers [9]. This is a remarkable result as we might naturally expect that as Alice's states become more and more thermalized secure transmission over any finite distance would become impossible. This further motivates an investigation of the security of CV-QKD as we move from optical frequencies into the infrared and down into the microwave region. As the wavelength gets longer there is no direct way of detecting single photons [10] thus ruling out discrete variable approaches. While CV measurements still apply, state preparation and the quantum channel become thermalized by the significant levels of background radiation that exist for longer wavelengths at room temperature. Here we show that CV-QKD remains, in principle, possible over short distances, well into the infrared and into the microwave regime. This surprising result highlights the possibility of short-range quantum cryptography applications at sub-optical frequencies.

Quantum Cryptography using Gaussian States - Typical Gaussian modulated CV-QKD protocols, begin with Alice randomly modulating a vacuum state to create a coherent state $|\alpha\rangle$ [11]. This random modulation or displacement $\alpha = Q_A + iP_A$ contains two independent variables $X_S \in \{Q_A, P_A\}$ chosen from a two-dimensional Gaussian distribution with variance V_S and zero mean. It is these continuous variables that will ultimately be used to construct a secret key between Alice and Bob. Alice then sends a whole ensemble of these randomly displaced pure coherent states to Bob over a quantum channel which is monitored by the eavesdropper, Eve. At the output of the channel, Bob measures the incoming states using either homodyne [4] or heterodyne detection [5].

The initial modes prepared by Alice can be described in the Heisenberg picture as $\hat{X}_A = X_S + \hat{X}_0$ where X_S describes the classical signal and $\hat{X}_0$ the thermal mode. Here the quadratures $\hat{Q}$ and $\hat{P}$ are defined as: $\hat{X}_A \in \{\hat{Q}_A, \hat{P}_A\}$ and $\hat{X}_0 \in \{\hat{Q}_0, \hat{P}_0\}$. The overall variance $V := V(\hat{X}_A)$ of Alice's initially prepared mode is given by: $V = V_S + V_0$. We can further decompose the variance of the thermal mode $V_0 := V(\hat{X}_0)$ into the variance of the pure vacuum mode (which is normalized to 1) and the variance of the unknown preparation noise at Alice's station β to give: $V_0 = 1+\beta$. Typically, in CV-QKD protocols, we simply have $V = V_S+1$, i.e., zero preparation noise ($\beta = 0$). In this paper, we consider the effect of having non-zero preparation noise on Alice's mode preparation, i.e., $\beta > 0$. We assume that this preparation noise cannot be controlled or manipulated by Eve.

In the analysis of CV-QKD protocols, the collective Gaussian attacks [12–14] are the most important. In fact, up to a suitable symmetrization of the protocols [15], these attacks bound the most powerful eavesdropping strategy allowed by quantum mechanics [15]. The most general form of a collective Gaussian attack is explicitly described in Ref. [14]. This consists in Eve interacting her (independent) ancilla modes with Alice and Bob's mode for each run of the protocol in such a way to generate a memoryless (one-mode) Gaussian channel. Eve's ancillas are then collected in a quantum memory whose measurement is optimized on Alice and Bob's classical communications [14]. For a practical implementation of the protocols, the most important collective Gaussian attack is the one based on the entangling cloner [16] which is exactly the model considered in our paper. This consists in Eve perfectly replacing the quantum channel between Alice and Bob with her own quantum channel where the loss is simulated by a beamsplitter with transmission T (which ranges in value from 0 to 1). She then creates her ancilla modes which are two-mode squeezed states [11] (or commonly known as, Einstein-Podolsky-Rosen (EPR) states), with variance W. The modes of the EPR beam can be described by the operators $\hat{E}''$ and $\hat{E}$. She keeps one mode of the beam $\hat{E}''$ and injects the other mode $\hat{E}$ into the unused port of the beamsplitter, resulting in the output mode $\hat{E}'$. Eve then collectively detects all modes $\hat{E}'$ and $\hat{E}''$, gathered from each of the runs of the protocol, in a final coherent measurement. The final stages of the protocol consists in Alice and Bob publicly revealing a subset of their data in order to estimate the channel transmission T and excess channel noise W [2]. We also assume that Alice and Bob (and Eve) know the variance of the unknown preparation noise β in order to properly estimate the channel noise as opposed to the sum of the channel noise and the preparation noise. However, the shot to shot displacement due to the excess preparation noise remains unknown to everyone. In the final steps of the protocol, Alice and Bob perform a reconciliation protocol (e.g., see [1]) to correct any errors they might have between them and then finally privacy amplification [2] to reduce Eve's knowledge of the key to a negligible, and safe amount.

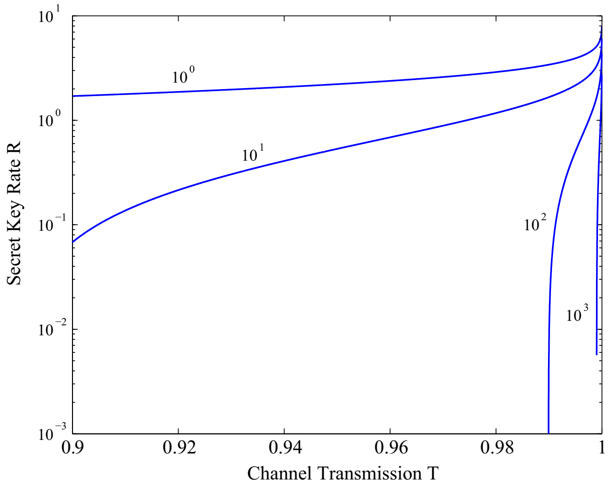

FIG. 1: Secret key rate $R^{\blacktriangleleft}$ versus channel transmission T using reverse reconciliation. Increasing the amount of unknown classical noise on Alice's preparation modes in CV-QKD. Here the thermal radiation is increased: $V_0 = 1, 10, 10^2, 10^3$ from left to right, where $W = 1$ (lossy channel), $V_S = 10^5$ and $V_0 = 1$ is a pure vacuum mode.

Reverse Reconciliation - We begin our analysis by first using the CV-QKD protocol known as reverse reconciliation [4] which consists in Alice (and Eve) optimally estimating Bob's measurement outcomes. We note that the previous analysis given in [9] also considered thermal state CV-QKD using reverse reconciliation. However, for completeness, we give the derivation for reverse reconciliation which will be helpful in calculating the direct reconciliation case and for a comparison between the two protocols. The secret key rate $R^{\blacktriangleleft}$ for reverse reconciliation where Bob uses homodyne detection is given by $R^{\blacktriangleleft} := I(X_A : X_B) - I(X_B : E)$. Here $I(X_A : X_B)$ is called the mutual information between Alice and Bob and defined in terms of the Shannon (or classical) entropy [17]. The quantum mutual information between Eve and Bob $I(X_B : E)$ is given by the Holevo information [18] and describes the most amount of information one can extract from a quantum state.

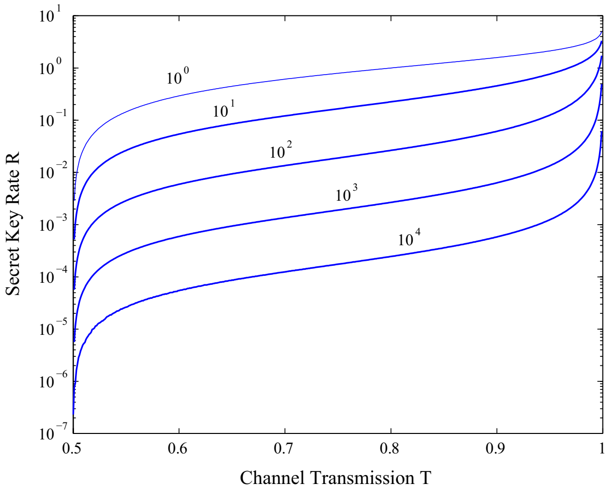

FIG. 2: Secret key rate $R^{\blacktriangleright}$ versus channel transmission T using direct reconciliation. Increasing the amount of unknown classical noise on Alice's preparation modes in CV-QKD. Here the thermal radiation is increased: $V_0 = 1, 10, 10^2, 10^3, 10^4$ from top to bottom, where $W = 1$, $V_S = 10^5$. We find that direct reconciliation does not show any deterioration in channel loss when excessively large amounts of preparation noise is added.

The secret key rate $R^{\blacktriangleleft}$ can be calculated (see Appendix for complete derivation) for various values of preparation noise, i.e., $V_0 = 1, 10, 100, 1000$. The results are plotted in Fig. 1 for a lossy channel (i.e., $W = 1$ which corresponds to Eve simply inserting a vacuum state into the unused port of the beamsplitter). We see that, as expected, the security is dependent on the channel transmission, and starts deteriorating rapidly as the excess preparation noise is increased. In fact, after only a modest increase in preparation noise (from $V_0 = 1$ to $V_0 = 10$), the secure region has shrunk to $T \approx> 0.89$.

Direct Reconciliation - We now turn our attention to another CV-QKD scheme known as direct reconciliation [3]. Direct reconciliation, was the first protocol to show that one could use Gaussian modulated coherent states to create a secure key. Unlike, reverse reconciliation, this protocol is a forward-way scheme where Bob (and Eve) are trying to optimally estimate the values of Alice's initial displacements, or encodings, Q_A and P_A. However, direct reconciliation has the drawback in its inability to create a secret key when the loss is greater than 3 dB. This corresponds to $T < 0.5$ and can be intuitively thought of as Eve sharing more common information with Alice than Bob does. Consequently, reverse reconciliation (or post-selection [7]) is usually considered the most practical CV-QKD protocol [19]. However, as we will see, despite these shortcomings, direct reconciliation offers a surprising advantage as a potential platform for *noise tolerant short-range QKD*.

The secret key rate $R^{\blacktriangleright}$ for direct reconciliation using homodyne detection is defined as $R^{\blacktriangleright} := I(X_A : X_B) - I(X_A : E)$ where $I(X_A : E)$ is again the Holevo quantity but now defined between Eve and Alice. We can now calculate the subsequent key rates (see Appendix for details). In Fig. 2 we have plotted the resulting secret key rates for various values of V_0 using $W = 1$ and $V_S = 10^5$. We find that direct reconciliation has the amazing feature that as the preparation noise becomes more and more significant (even up to 10^4 times that of the variance of the pure vacuum mode) only the secret key rate decreases and *not* the channel transmission. So for any value of preparation noise the initial starting point is always $T = 0.5$ (c.f. reverse reconciliation where modest increases in noise reduce the secure region close to unity transmission, i.e., see Fig. 1). The basic physics is that, for $T > 0.5$, the presence of quantum noise always gives Alice and Bob a direct information advantage over Eve. Increased preparation noise reduces this advantage, but it always remains finite. In contrast, for reverse reconciliation, Alice's ability to estimate what Bob received is rapidly compromised by the preparation noise. This removes their information advantage over Eve.

In Fig. 3 we have a security threshold plot for direct and reverse reconciliation for $W = 1$. The solid (blue) curve is the previous best bound derived using reverse reconciliation and is given by [9]: $\beta < (1 - T)^{-1}$. On the same plot we have the new direct reconciliation bound which shows a substantial improvement over the previous reverse reconciliation bound. Remarkably, we can see how direct reconciliation is unaffected by the channel transmission once $T > 0.5$ and is secure for a *minimum* of 4 orders of magnitude of preparation noise. Therefore, it is best to use reverse reconciliation when $T \leq 0.5$ and direct reconciliation when $T > 0.5$. Additionally, this result is robust to the addition of small amounts of excess noise on the quantum channel (i.e., $W > 1$) which moves the transmission limit slightly over 50% but retains qualitatively the same behavior as the lossy case [20].

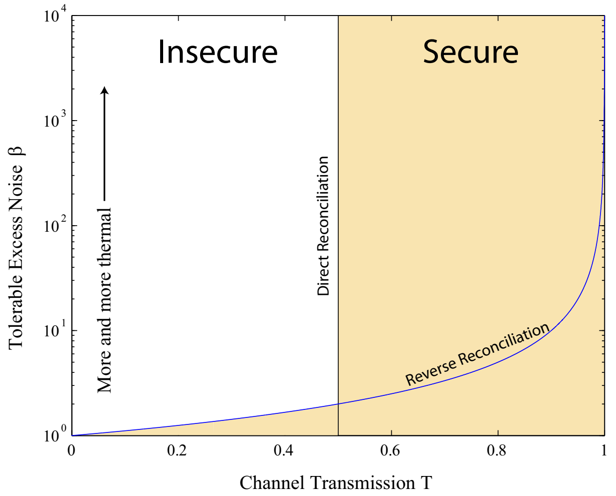

FIG. 3: Tolerable preparation (classical) excess noise $\beta = V_0 - 1$ versus channel transmission T for direct and reverse reconciliation over a lossy channel. The area under the solid (blue) curve indicates the previous best secure region threshold using reverse reconciliation [9]. However, for direct reconciliation, after $T = 0.5$, one can immediately obtain many orders of magnitude improvement in the security threshold.

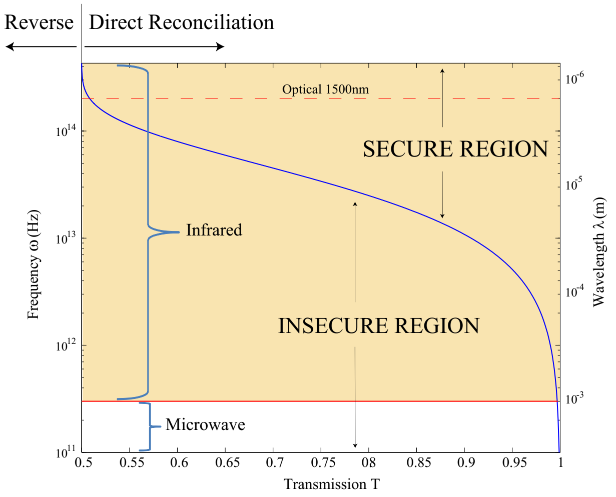

FIG. 4: Security of quantum cryptography over various electromagnetic wave frequencies (at room temperature) as a function of channel transmission. Moving our way from the infrared spectrum (430 THz) and into the microwave spectrum (300 GHz). Our results show that direct reconciliation should be used when channel losses are less than 50% and reverse reconciliation otherwise. We note that at each point the same impurity applies to both Alice and Eve with $V_S = 10^8$.

Infrared to Microwave Quantum Cryptography - It is interesting to consider a possible application of our results: wireless CV-QKD at infrared to microwave frequencies. Today, a large number of popular wireless communication technologies rely on such frequencies to distribute information. Due to the ubiquitous nature of such devices, their security is of fundamental importance. Moving to frequencies lower than optical rules out discrete variable QKD because of the lack of photon counting capabilities. The problem for CV-QKD is that operating at lower frequencies at room temperature inevitably introduces a significant amount of thermal noise. In contrast to the previous section, we now consider a simplified wireless communication protocol where *both* Alice's preparation modes and the quantum channel (Eve) are affected by the thermal background. When considering Eve we assume that she prepares her attack within a cryostat which allows her to essentially prepare pure modes away from the effect of the background radiation. Then to cover her tracks she adds *known* excess noise to her pure states to emulate the thermal noise of the environment.

In the previous section we showed that direct reconciliation is significantly more robust against preparation noise than reverse reconciliation and is consequently better suited to our current analysis. Given that, the next step is to calculate how strong the thermal modes are at particular frequencies from optical down to the microwave (1 GHz ($\lambda = 30$ cm) to 300 GHz ($\lambda = 1$ mm)). To do this we first write the average photon number $\bar{n}$ in terms of the quadrature variance V using $\bar{n} = \langle \hat{a}^\dagger \hat{a} \rangle = (V-1)/2 \implies V = 2\bar{n}+1$ where we have symmetrized both quadratures, i.e., $V := V(\hat{Q}) = V(\hat{P})$ and the annihilation operator $\hat{a}$ is defined as $\hat{a} = (\hat{Q}+i\hat{P})/2$. Secondly, the average photon number is equal to $\bar{n} = [\exp(\hbar\omega/k_B T) - 1]^{-1}$ [11] and represents the blackbody radiation spectrum. For example, at room temperature $T = 300$ K and using a microwave frequency of $\omega = 1$ GHz we find that the variance of the thermal mode is $V = 7.85 \times 10^4$; while at the other end of the microwave spectrum ($\omega = 300$ GHz) the variance is $V = 2.63 \times 10^2$.

Using the analysis from the previous section, we can calculate the secret key rates using direct reconciliation. In Fig. 4 we plot the security of CV-QKD from the optical frequency (1550 nm) into the infrared region and down into the microwave frequency as a function of channel line transmission. We point out that the secure region corresponds to $R > 0$. We find a window of security for CV-QKD throughout all of the infrared region and into the microwave frequency albeit with smaller allowed levels of loss. In the mid-infrared region transmission of $T \approx 0.8$ is required whilst in the case of the microwave region we see that a secure key can only be generated when the transmission is higher than $T \approx 0.9969$. Nonetheless, it is interesting that a small security window, in principle, exists. Future analysis will look at improving the region where infrared and microwave CV-QKD is secure. For example, in [6] they showed that the security thresholds for direct reconciliation could be improved (and in fact beat the 3 dB loss limit) if two-way quantum communication was used. Furthermore, post-selection [7] could also be used to investigate a possible way to combat the high preparation noise.

Conclusion - In conclusion, we have shown that when considering unknown preparation noise in continuous-variable QKD, direct reconciliation is significantly more robust than reverse reconciliation when the channel loss does not exceed 50%. Incredibly, direct reconciliation showed no deterioration in the loss threshold, only in secret key rates, even when the variance of the thermal noise is as much as 10^4 times greater than that of the pure vacuum mode. Furthermore, we have shown that infrared to microwave quantum cryptography is, in principle, possible over short distances when using continuous variables and opens up the possibility of further avenues of investigations. In conclusion, we have shown that when considering unknown preparation noise in continuous-variable QKD, direct reconciliation is significantly more robust than reverse reconciliation when the channel loss does not exceed 50%. Incredibly, direct reconciliation showed no deterioration in the loss threshold, only in secret key rates, even when the variance of the thermal noise is as much as 10^4 times greater than that of the pure vacuum mode. Furthermore, we have shown that infrared to microwave quantum cryptography is, in principle, possible over short distances when using continuous variables and opens up the possibility of further avenues of investigations.

Acknowledgments – C. W. and T. R. would like to thank the Australian Research Council (ARC) for funding. S. P. was supported by a Marie Curie Action of the European Community. S. L. and C. W. would like to thank the W. M. Keck Foundation Center for Extreme Quantum Information Theory for funding. C.W. would also like to thank Vladyslav Usenko, Radim Filip, Warwick Bowen, Nathan Walk, Denis Sych, Franco Wong, Travis Humble and Jeff Shapiro for helpful discussions.

APPENDIX

Introduction to Gaussian Formalisms

Here we introduce some of the Gaussian tools and techniques required for our analysis. Such Gaussian formalisms can be found elsewhere in the literature typically in the context of *quantum information using continuous variables* (for example, see [6, 21–23]). However, in what follows, we give the reader a self-contained treatment for what is needed to understand and derive the results given in the main text of the paper.

To begin with, we can define the quadrature row vector $\hat{\mathbf{Y}}$, which describes a bosonic system [24] of n modes, as:

$$\hat{\mathbf{Y}} = (\hat{Q}_1, \hat{P}_1, ..., \hat{Q}_n, \hat{P}_n), \tag{1}$$

where $\hat{Y}_l$ is the lth element of the vector. This satisfies the commutator relation:

$$[\hat{Y}_l, \hat{Y}_m] = 2i\Omega_{lm}, \tag{2}$$

for $1 \leq l, m, \leq 2n$. Here the matrix $\mathbf{\Omega}$ defines the symplectic form and is given as

$$\mathbf{\Omega} := \bigoplus_{k=1}^{n} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \tag{3}$$

where Ω_{lm} denote the row l and column m of the matrix, e.g., Ω_{11} is the first row and first column entry of Ω. Firstly, the notation for the above matrix can be explained with a simple example. For $n = 2$ mode case the direct sum $\bigoplus$ means that we form two 2×2 block diagonal matrices to create a larger 4×4 matrix, i.e.,

$$\mathbf{\Omega}_{n=2} := \bigoplus_{k=1}^{2} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \left(\begin{array}{cc|cc} 0 & 1 & & \\ -1 & 0 & & \\ \hline & & 0 & 1 \\ & & -1 & 0 \end{array} \right), \tag{4}$$

where the empty spaces indicate zero elements. Secondly, the compact version of the commutator given in Eq. (2) can now be understood using the simple case of one mode ($n = 1$) where

$$\mathbf{\Omega}_{n=1} := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \tag{5}$$

and $\hat{Y}_1 := \hat{Q}_1$ and $\hat{Y}_2 := \hat{P}_1$ for $l, m = 1, 2$. Therefore Eq. (2) is a compact way of saying the following:

$$\begin{aligned}
[\hat{Y}_1, \hat{Y}_1] &= [\hat{Q}_1, \hat{Q}_1] = 2i\Omega_{11} = 0, \\
[\hat{Y}_1, \hat{Y}_2] &= [\hat{Q}_1, \hat{P}_2] = 2i\Omega_{12} = 2i, \\
[\hat{Y}_2, \hat{Y}_1] &= [\hat{P}_2, \hat{Q}_1] = 2i\Omega_{21} = -2i, \\
[\hat{Y}_2, \hat{Y}_2] &= [\hat{P}_2, \hat{P}_2] = 2i\Omega_{22} = 0.
\end{aligned} \tag{6}$$

A Gaussian bosonic state ρ is fully characterized by its displacement

$$\langle \hat{\mathbf{Y}} \rangle = \mathrm{Tr}(\hat{\mathbf{Y}}\rho), \tag{7}$$

and its correlation matrix (CM). The various elements of a correlation matrix **V** can be calculated using the following formulas. Firstly, the off-diagonal terms:

$$V_{lm} := \frac{1}{2}\langle \hat{Y}_l \hat{Y}_m + \hat{Y}_m \hat{Y}_l \rangle - \langle \hat{Y}_l \rangle \langle \hat{Y}_m \rangle, \tag{8}$$

and the diagonal elements:

$$V_{ll} = \langle \hat{Y}_l^2 \rangle - \langle \hat{Y}_l \rangle^2 := V(\hat{Y}_l). \tag{9}$$

Qualitatively it means that the diagonal terms contain the variances whilst the off-diagonal terms contain the correlations. An example might help here. A simple vacuum state, where the variance of the quadratures is normalized to one, has a CM given by

$$\mathbf{V}_{vac} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{10}$$

We can see that the variance of each quadrature is on the diagonal, whilst on the off-diagonal we have the zero correlation (meaning they are independent) terms.

The von Neumann entropy [25]

$$S(\rho) = -\mathrm{Tr}(\rho \log_2 \rho), \tag{11}$$

of a Gaussian state ρ can be written in terms of its *symplectic eigenvalues* ν_k as [26]

$$S(\rho) = \sum_{k=1}^{n} g(\nu_k), \tag{12}$$

where

$$g(\nu) := \Big(\frac{\nu+1}{2}\Big)\log_2\Big(\frac{\nu+1}{2}\Big) - \Big(\frac{\nu-1}{2}\Big)\log_2\Big(\frac{\nu-1}{2}\Big). \tag{13}$$

These symplectic eigenvalues can be calculated using the formula

$$\nu = |i\mathbf{\Omega}\mathbf{V}|, \tag{14}$$

where $\nu \geq 1$. The above notation means that you first find the eigenvalues of the matrix $i\mathbf{\Omega}\mathbf{V}$ and then take the absolute values. As it turns out these eigenvalues (known also as the symplectic spectrum) are a powerful tool which allows one to determine many important features of a Gaussian system. Although Eq. (14) gives one a way of calculating the spectrum, the output from using such a formula can sometimes lead very complicated equations. In certain circumstances, we are able to simplify the calculation of the eigenvalues. Let's look at that now. First, consider a generic two-mode CM in block form

$$\mathbf{V} = \begin{pmatrix} \mathbf{A} & \mathbf{C} \\ \mathbf{C}^T & \mathbf{B} \end{pmatrix}. \tag{15}$$

It is known [27] that its symplectic eigenvalues ν_1 and ν_2 can be written in the form

$$\nu_{1,2} = \sqrt{\frac{1}{2}\Big(\Delta \pm \sqrt{\Delta^2 - 4\det\mathbf{V}}\Big)}, \tag{16}$$

where $\det\mathbf{V}$ means the determinant of the matrix **V** and

$$\Delta := \det\mathbf{A} + \det\mathbf{B} + 2\det\mathbf{C}. \tag{17}$$

In particular, let us consider a CM of the form

$$\mathbf{V} = \begin{pmatrix} a\mathbf{I} & \sqrt{T}c\mathbf{Z} \\ \sqrt{T}c\mathbf{Z} & b\mathbf{I} \end{pmatrix}, \tag{18}$$

where $c \geq 0$, $T \in [0, 1]$ and

$$\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \mathbf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{19}$$

We can easily verify that $\det\mathbf{V} = (ab - c^2T)^2$ and $\Delta = a^2 + b^2 - 2c^2T$. As a consequence, the eigenvalues take the simple expression

$$\nu_{1,2} := \frac{1}{2}\Big(\sqrt{y} \pm (a-b)\Big), \tag{20}$$

where $y := (a+b)^2 - 4c^2T \geq 4$.

Reverse Reconciliation

The secret key rate $R^{\blacktriangleleft}$ for reverse reconciliation where Bob uses homodyne detection is given by

$$R^{\blacktriangleleft} := I(X_A : X_B) - I(X_B : E), \tag{21}$$

where $I(X_A : X_B)$ is known as the mutual information between Alice and Bob and $I(X_B : E)$ the mutual information between Bob and Eve. We have a secure key when the key rate is positive, i.e.,

$$R > 0. \tag{22}$$

Another way to think about this is a secure key can be synthesized when Eve has less information than Alice and Bob:

$$I(X_A : X_B) > I(X_B : E). \tag{23}$$

We also note that, for Alice and Bob, the variable $\hat{X}$ corresponds to either of the two quadratures $\{\hat{Q}, \hat{P}\}$, such that

$$\hat{X}_A = \{\hat{Q}_A, \hat{P}_A\}, \tag{24}$$

$$\hat{X}_B = \{\hat{Q}_B, \hat{P}_B\}. \tag{25}$$

Firstly, let us calculate the mutual information between Alice and Bob where

$$I(X_A : X_B) := H(X_B) - H(X_B|X_A). \tag{26}$$

Here

$$H(X_B) = \frac{1}{2}\log_2 V(\hat{X}_B), \tag{27}$$

is the Shannon (or classical) entropy and

$$H(X_B|X_A) = \frac{1}{2}\log_2 V(\hat{X}_B|X_A), \tag{28}$$

is known as the conditional Shannon entropy [17]. To determine $\hat{X}_B$ we set up a generic quantum channel with transmission $T \in [0, 1]$ with excess noise $\hat{N}$ and model it using a beamsplitter equation, where the transmitted output (received by Bob) is given by:

$$\hat{X}_B = \sqrt{T}\hat{X}_A + \sqrt{1-T}\hat{N}. \tag{29}$$

The variance of the above equation is given by

$$V(\hat{Q}_B) = V(\hat{P}_B) = (1-T)W + TV := b_V, \tag{30}$$

where both quadratures have been symmetrized and $V(\hat{N}) := W$. Also, the variance of Alice's modes is given by

$$V = V_S + V_0, \tag{31}$$

where V_S is the variance of the initial signal encodings and V_0 is the variance of the vacuum state (see main text for more detail). In Eq. (28) the conditional variance term $V(\hat{X}_B|X_A)$ is derived by setting up an optimal estimator equation (e.g., see its use in [6] or [28]):

$$V(\hat{X}_B|X_A) = V(\hat{X}_B) - \frac{|\langle\hat{X}_B X_S\rangle|^2}{V(X_S)}, \tag{32}$$

where specifically here we have $X_S \in \{Q_A, P_A\}$ (the signal) rather than $\hat{X}_A$ (signal plus noise) because it is Bob's estimate of Alice's signal not his estimate of both the signal and noise. Calculating this explicitly we get:

$$V(\hat{Q}_B|Q_A) = V(\hat{P}_B|P_A) = (1-T)W + TV_0 := b_1. \tag{33}$$

Using Eq. (26) with Eqs. (27) and (28) we calculate Alice and Bob's mutual information to be

$$I(X_A : X_B) = \frac{1}{2}\log_2\Big[\frac{(1-T)W + TV_S + TV_0}{(1-T)W + TV_0}\Big]. \tag{34}$$

We now turn our attention to calculating the mutual information between Eve and Bob. This is given by the Holevo information [18] defined as

$$I(X_B : E) := S(E) - S(E|X_B). \tag{35}$$

In the literature it is also common to use the notation χ for the Holevo (information) bound (for more background on both the classical and quantum information formulas, see e.g., [25, 29]).

Here the quantum entropies $S(E) := S(\rho_E)$ and $S(E|X_B)$ are found by calculating the eigenvalues, or symplectic spectrum ν, of their corresponding CMs: $\mathbf{V}_E$ and $\mathbf{V}_{E|X_B}$, respectively. Eve's CM is made up from the two modes $\hat{E}'$ and $\hat{E}''$ (see main text for details) and is given by

$$\mathbf{V}_E(V, V) = \begin{pmatrix} \mathbf{\Delta}[e_V, e_V] & \varphi\mathbf{Z} \\ \varphi\mathbf{Z} & W\mathbf{I} \end{pmatrix}, \tag{36}$$

where

$$e_V := (1-T)V + TW, \tag{37}$$

and the notation $\mathbf{\Delta}[\cdot,\cdot]$ simply means a diagonal matrix with the arguments $[\cdot,\cdot]$ on the diagonal entries and also

$$\varphi = [T(W^2-1)]^{1/2}. \tag{38}$$

Eve's symplectic spectra can be determined by using Eq. (20)

$$\nu_E = \frac{1}{2}[\sqrt{(e_V+W)^2 - 4T(W^2-1)} \pm (e_V - W)]. \tag{39}$$

Eve's conditional CM is given by

$$\mathbf{V}_{E|X_B} = \mathbf{V}_E - (\beta_V)^{-1}\mathbf{C}\mathbf{\Pi}\mathbf{C}^T, \tag{40}$$

where $\mathbf{V}_E$ is defined in Eq. (36) and

$$\mathbf{\Pi} := \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}. \tag{41}$$

Furthermore, $\mathbf{C}$ is a 4×2 matrix describing the quantum correlations between Eve's modes $\{\hat{E}', \hat{E}''\}$ and Bob's output mode $\hat{X}_B$ and is defined as

$$\mathbf{C} := \begin{pmatrix} \langle\hat{E}'\hat{X}_B\rangle\mathbf{I} \\ \langle\hat{E}''\hat{X}_B\rangle\mathbf{Z} \end{pmatrix} = \begin{pmatrix} \xi\mathbf{I} \\ \phi\mathbf{Z} \end{pmatrix}, \tag{42}$$

where

$$\xi = \sqrt{T(1-T)}(V_S + V_0 - W), \tag{43}$$

and

$$\phi = \sqrt{1-T}\sqrt{W^2-1}, \tag{44}$$

and we have used

$$\hat{X}_B = \sqrt{T}\hat{X}_A + \sqrt{1-T}\hat{E}, \tag{45}$$

and

$$\hat{E}' = \sqrt{1-T}\hat{X}_A - \sqrt{T}\hat{E}. \tag{46}$$

Using the above we find that Eve's conditional CM $\mathbf{V}_{E|X_B}$ has the form

$$\mathbf{V}_{E|X_B} = \begin{pmatrix} \mathbf{A} & \mathbf{C} \\ \mathbf{C}^T & \mathbf{B} \end{pmatrix}, \tag{47}$$

where

$$\mathbf{A} = \begin{pmatrix} \frac{VW}{T(V-W)+W} & 0 \\ 0 & (1-T)V+TW \end{pmatrix}, \tag{48}$$

$$\mathbf{B} = \begin{pmatrix} \frac{1-T+TWV}{TV+W-TW} & 0 \\ 0 & W \end{pmatrix},$$

$$\mathbf{C} = \begin{pmatrix} \sqrt{T(W^2-1)}\left[2 - \frac{V}{TV+W-TW}\right] & 0 \\ 0 & -\sqrt{T(W^2-1)} \end{pmatrix}.$$

Using Eq. (16) the corresponding symplectic spectra $\nu_{E|X_B}$ of $\mathbf{V}_{E|X_B}$ can be calculated where

$$\Delta = \Big[W + V^2W - 4T^2(V-W)(W^2-1) \\ - T(2V + (V^2-3)W - 4VW^2 + 4W^3)\Big]/[T(V-W)+W], \tag{49}$$

and

$$\det\mathbf{V}_{E|X_B} = \Big[(-T + (T-1)VW)(-4(T-1)TW(W^2-1) \\ + V(-1 + 4(T-1)T(W^2-1))\Big]/[T(V-W)+W]. \tag{50}$$

The final secret key rate $R^{\blacktriangleleft}$ can now be calculated numerically, using Eq. (21) with the appropriate formulas, for various values of preparation noise.

Direct Reconciliation

The secret key rate $R^{\blacktriangleright}$ for direct reconciliation using homodyne detection is given by

$$R^{\blacktriangleright} := I(X_A : X_B) - I(X_A : E), \tag{51}$$

where $I(X_A : X_B)$ has already been calculated in Eq. (34). For Eve, we have

$$I(X_A : E) := S(E) - S(E|X_A), \tag{52}$$

where again we have already calculated $S(E)$ previously and $S(E|X_A)$ is calculated from the spectrum of the conditional CM $\mathbf{V}_{E|X_A}$. Eve's conditional CM for homodyne detection using direct reconciliation is equal to

$$\mathbf{V}_{E|Q_A} = \mathbf{V}_E(V_0, V), \tag{53}$$

where $\mathbf{V}_E$ is defined in Eq. (36). Using Eq. (14) the corresponding symplectic spectra $\nu_{E|X_A}$ is:

$$\nu_{E|X_A} = \frac{1}{\sqrt{2}}\Big(\sqrt{|F \pm \sqrt{G}|}\Big) \tag{54}$$

where

$$F = VV_0 + T(2 + (T-2)VV_0) - TW(T-1)(V+V_0) \\ + W^2(T-1)^2, \tag{55}$$

and

$$G = (T-1)^2(T^2(V-W)^2(V_0-W)^2 + (-V_0V + W^2)^2 \\ + 2T(V-W)(W-V_0)(-2 + VV_0 + W^2)). \tag{56}$$

The final secret key rate $R^{\blacktriangleright}$ can now be calculated numerically, using Eq. (51) with the appropriate formulas, for various values of preparation noise.

---

[*] Electronic address: christian.weedbrook@gmail.com

[1] N. J. Cerf and Ph. Grangier, J. Opt. Soc. Am. B **24**, 2 (2007).
[2] V. Scarani *et al.*, Rev. Mod. Phys. **81**, 1301 (2009).
[3] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
[4] F. Grosshans *et al.*, Nature **421**, 238 (2003).
[5] C. Weedbrook *et al.*, Phys. Rev. Lett. **93**, 170504 (2004).
[6] S. Pirandola *et al.*, Nature Physics 4, **726** (2008).
[7] C. Silberhorn *et al.*, Phys. Rev. Lett. **89**, 167901 (2002).
[8] A. M. Lance *et al.*, Phys. Rev. Lett. **95**, 180503 (2005).
[9] R. Filip, Phys. Rev. A **77**, 022310 (2008); V. C. Usenko and R. Filip, Phys. Rev. A **81**, 022318 (2010).
[10] G. Temporão, *et al.*, Opt. Lett. **31**, 1094 (2006).
[11] C. C. Gerry and P. L. Knight, *Introductory Quantum Optics*, Cambridge, (2005).
[12] M. Navascués, F. Grosshans, and A. Acín, Phys. Rev. Lett. **97**, 190502 (2006).
[13] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006).
[14] S. Pirandola et al., Phys. Rev. Lett. **101**, 200504 (2008).
[15] R. Renner and J. I. Cirac, Phys. Rev. Lett. **102**, 110504 (2009).
[16] F. Grosshans *et al.*, Quantum. Inf. Comput. **3**, 535 (2003).
[17] C. E. Shannon, Bell Syst. Tech. J. **27**, 623656 (1948).
[18] A. S. Holevo, Probl. Inf. Transm. **9**, 177-183 (1973).
[19] A. Leverrier and Ph. Grangier, Phys. Rev. Lett. **102**, 180504 (2009).

[20] C. Weedbrook *et al.*, (to be published).

[21] A. Ferraro, S. Olivares, M. G. A. Paris, arXiv:quant-ph/0503237 (2005).

[22] G. Adesso, Ph.D. thesis, Univerità Degli Studi Di Salerno, 2006.

[23] R. Garcia-Patron, Ph.D. thesis, Université Libre de Bruxelles, 2007.

[24] S. L. Braunstein and P. van Loock, Rev. Mod. Phys. **77**, 513 (2005).

[25] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).

[26] A. S. Holevo, M. Sohma, and O. Hirota, Phys. Rev. A **59**, 1820 (1999).

[27] A. Serafini *et al.*, J. Phys. B: At. Mol. Opt. Phys. **37**, L21 (2004); S. Pirandola, A. Serafini, and S. Lloyd, Phys. Rev. A **79**, 052327 (2009).

[28] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph and P. K. Lam, Phys. Rev. A **73**, 022316 (2006).

[29] T. M. Cover and J. A. Thomas, *Elements of information theory* (Wiley-Interscience, New York, 2006).